

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

ERIKA LEE,

Plaintiff,

v.

DELTA AIR LINES, INC., DAVID
NEEDHAM, and JOSE ROSADO,

Defendants.

22-CV-8618 (DEH) (RWL)

ELECTRONIC DISCOVERY ORDER

WHEREAS, Defendant Delta Air Lines, Inc. (“Defendant” or “Delta”) requests that this Court issue an order pursuant to Rule 26(c) of the Federal Rule of Civil Procedure to manage the exchange of electronically stored information (“ESI”) in the pretrial phase of this action;

WHEREAS, the Court finds that good cause exists for issuance of an appropriately tailored electronic discovery order (the “Electronic Discovery Order”) governing the treatment of ESI exchanged in the pretrial phase of this action,

IT IS HEREBY ORDERED that the following specifications shall govern discovery of ESI during discovery in the above-captioned action.

I. General

A. The terms of this Electronic Discovery Order shall be construed to ensure the exchange of information consistent with the Federal Rules of Civil Procedure, the Local Rules, and any other orders by this Court.

B. This Electronic Discovery Order shall not enlarge, reduce, or otherwise affect the scope of discovery in this action as imposed by the Federal Rules of Civil Procedure, the Local Rules, and any other orders of the Court.

C. Nothing in this Electronic Discovery Order shall be interpreted to require disclosure of materials that a Party contends are not discoverable or are protected from disclosure by the attorney-client privilege, the attorney work product doctrine, or any other privilege that may be applicable.

D. Nothing in this Electronic Discovery Order shall be deemed to waive or limit any Party's right to object to the production of certain ESI or to move for an appropriate order pursuant to the Federal Rules of Civil Procedure on the ground that the sources are not reasonably accessible because of undue burden or cost or on the ground that there is good cause for the document's production.

E. Consistent with their obligations under applicable Federal Rules of Civil Procedure, the Parties will attempt to resolve, in person, in writing (including e-mail) or by telephone, disputes regarding the issues set forth herein prior to filing a motion with the Court, or otherwise seeking relief. If the Parties are unable to resolve the dispute after a good faith effort, the Parties may seek Court intervention in accordance with the Court's procedures.

II. Production Format

A. File Types and Formats. Emails shall be produced as PDFs. A Party may, in its discretion produce spreadsheet files (*e.g.*, Microsoft Excel, Corel Quattro, etc.) as PDFs or as native files with PDF placeholder images. Except as otherwise stated herein, audio files (*e.g.*, .mp3, .mp4, .wav, etc.), and video files (*e.g.*, .wvm, .m4v, etc.) shall be produced as native files

with PDF placeholder images. The Parties will meet and confer on the production of other file types, as necessary.

B. Images. ESI should be produced as PDFs except for those documents detailed in Section II(A). PDFs shall be named according to the Bates number, and Bates numbers and confidentiality designations, if applicable, should be electronically branded on each produced image. Color originals may be produced in B&W, but either Party may subsequently request, by Bates number(s), a replacement set of images in color only to the extent that the Requesting Party demonstrates that the loss of the color detracts from the usability or reduces the ability to understand the information imparted in the original, however categorical or wholesale requests are deemed invalid.

C. Parent-Child Relationships. Unless otherwise addressed in this Electronic Discovery Order, for email families, the parent-child relationships (the association between emails and attachments) should be preserved. Email attachments should be consecutively produced with parent email record.

D. Metadata to Be Produced. To the extent that metadata does not exist, is not reasonably accessible or available for any documents produced, or would be overly burdensome to provide, nothing in this Electronic Discovery Order shall require any Party to extract, capture, collect or produce such data.

E. Native Files. If a document is produced in native format, a single-page Bates-stamped PDF image slip-sheet containing the confidential designation and text stating the document has been produced in native format should also be provided. Each native file should be named according to the Bates number it has been assigned. If documents requested in native format

require redactions, the Parties should meet and confer regarding how to implement redactions while ensuring that proper formatting and usability are maintained. To the extent that either Party believes that native files should be produced for a specific document or class of documents not required to be produced in native format pursuant to this paragraph or to the extent records do not easily conform to native or PDF format (*i.e.*, structured data), the Parties should meet and confer in good faith.

F. Limited Informal Electronic Collection. Defendant may collect and produce certain categories of documents utilizing informal collection methods even though such collection method may alter certain aspects of those files' metadata as they exist at the time of collection (e.g., created date, file path).

III. Previously Collected and Produced Data

This Electronic Discovery Order does not create an obligation to recollect or reproduce any prior collections or productions collected or produced prior to the entry of this Electronic Discovery Order. This includes not requiring either Party to reproduce productions in the production format outlined in this Electronic Discovery Order.

IV. Production – Receipt and Storage of ESI

The recipient of any ESI that is provided under this Electronic Discovery Order shall maintain such information in a reasonably secure and safe manner that ensures access is limited to the persons authorized herein, and shall further exercise the same standard of due and proper care with respect to the storage, custody, use, and/or dissemination of such information as the recipient would use with respect to its own proprietary information.

If the recipient discovers any loss of ESI or a breach of security, including any actual or suspected unauthorized access, relating to the produced ESI, the Receiving Party shall:

A. Promptly provide written notice to Producing Party of such breach within a reasonable time of the breach discovery.

B. Investigate and make reasonable efforts to remediate the effects of the breach and provide Producing Party with assurances that safeguards are being implemented to ensure another breach does not occur.

C. Provide sufficient information about the breach that the Producing Party can reasonably ascertain the size and scope of the breach. The Requesting Party agrees to cooperate with the Producing Party or law enforcement in investigating any such security incident.

D. The Requesting Party shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access and/or correct the breach.

V. Production Format - Structured Data

If a Party is producing electronic information from a database that cannot be provided in a readily accessible production format (e.g., as an Excel file), the Parties will meet and confer in advance of that production to discuss the most appropriate and cost-effective production format, which may include an export of data. The Parties will reasonably cooperate in the exchange of information concerning such databases to facilitate discussions on productions and production format. If the Parties cannot reach agreement, the Parties may refer the matter to the Court or its designee.

VI. Production Format – Social Media

If a Party is producing electronic information from social media websites (e.g., LinkedIn, Facebook, Twitter), the Parties will meet and confer in advance of that production to discuss the most appropriate and cost-effective production format.

VII. Production Format - Media

Documents shall be exchanged on secure file transfer protocols (e.g., FTP) or similar secure electronic transmission. The production media shall be labeled with the Volume Number along with the Bates Number range(s) of the materials, and where not practicable to do so, may be provided in an accompanying letter.

VIII. Processing and Other Specifications

A. Bates Numbering and Confidentiality Designations. Each page of a produced image shall have a legible, unique Bates number that includes an alpha prefix along with a fixed number, e.g., ABC00000001, electronically “burned” onto the image at the bottom of the page so as not to unreasonably obscure any information from the source document. Each image page or native file assigned a Bates number shall be assigned a Bates number that is unique and maintains a constant length across the entire document production. No other legend or stamp will be placed on the document image other than confidentiality legends (where applicable) or redactions.

B. ESI Date and Time Processing. Each Party’s ESI should be processed using a consistent Time Zone for all data. The Party shall share the Time Zone selected for processing of its data with the other Party.

C. Global or Horizontal Deduplication. Removal of duplicate documents should only be done on exact duplicate documents (based on MD5 or SHA-1 hash values, at the family level).

Attachments should not be eliminated as duplicates for purposes of production, unless the parent e-mail and all attachments are also duplicates. An email that includes content in the BCC or other blind copy field should not be treated as a duplicate of an email that does not include content in those fields, even if all remaining content in the email is identical.

D. To the extent a Party identifies identical documents where the hash values do not match as a result of technical issues due to emails being stored in and collected from two email environments, the Producing Party can use near duplicate analysis to remove documents with 100% textual matches.

E. Email Thread Suppression: Each Party may deduplicate e-mails in such a way as to eliminate earlier or incomplete chains of e-mails, and produce the email that contains the most complete iteration of an e-mail chain — i.e., the produced email contains all previous replies, forwards, and the original message and all attachments in the whole email family. A Party may, therefore, not eliminate earlier emails that have attachments not attached to the last email in a chain. However, a Party may not create a new thread by combining related emails if such emails are not contained in one already existing email.

F. Redactions. As described in more detail below, the Producing Party can redact non-public personally identifiable information and material that is claimed to be privileged. If, during the course of discovery, the Parties identify other kinds of information that any Party has a reasonable basis for redacting, the Parties will meet and confer regarding it before such redactions are made. If the issue cannot be resolved, the Parties may seek resolution from the Court.

G. No Designation of Discovery Requests. Production of ESI in the reasonably usable form set out in this Electronic Discovery Order need not include any reference to the requests to which a document or ESI may be responsive.

H. Foreign Language Documents. To the extent that ESI is produced that contain languages other than English, in whole or in part, the Producing Party shall produce all foreign language document and ESI in the original language. Documents containing foreign language text must be OCR'd using the appropriate settings for that language (e.g., OCR of German documents must use settings that properly capture umlauts and OCR of Asian language documents must properly capture the relevant Asian characters). The Producing Party has no obligation to provide a translation of the documents or ESI or any portion thereof.

IX. Identification and Collection of Documents

A. The Producing Party must make reasonable efforts to select and/or propose custodians who likely possess information and documents responsive to the respective discovery demands.

B. Search Methodology.

1. Email and Non-Email. The Parties agree to search for and produce unique, responsive records from sources of ESI to the extent a custodian reveals that such locations may contain responsive information and such data is within the possession, custody or control of the Producing Party.

2. The mere fact that a document is hit or captured by the application of any agreed upon search terms does not mean that such document is necessarily responsive to any

propounded discovery request or is otherwise relevant to this litigation. Determinations of discoverability, responsiveness and privilege shall be made by the Producing Party.

X. Preservation

A. The Parties acknowledge that they have an obligation to take reasonable and proportional steps to preserve discoverable information in the Party's possession, custody or control.

B. The Parties agree that the circumstances of this case do not warrant the preservation, collection, review, or production of the following sources of ESI because they are either not reasonably accessible or not likely to contain additional relevant information from other sources whereby the associated burden and costs outweigh any benefit:

1. Data duplicated in any electronic backup system.
2. Deleted, shadowed, damaged, residual, slack, fragmented, or other data only accessible by forensics and "unallocated" space on hard drives.
3. Data stored in random access memory ("RAM"), temporary files, or other ephemeral data that is difficult to preserve without disabling operating systems.
4. On-line access data such as temporary internet files, history, cache files, cookies, and the like, wherever located.
5. Data stored on photocopiers, scanners and fax machines.
6. Data in metadata fields that are frequently updated automatically, such as last-opened dates.

7. Server, system or network logs.
8. Legacy data or data remaining from systems no longer in use that is unintelligible on the systems in use to the extent such data is duplicative of data on systems in use.
9. Computer programs, operating systems, computer activity logs, programming notes or instructions, batch files, system files, and miscellaneous files or file fragments.
10. Data stored on mobile devices (excluding laptop and notebook computers) and tablets.

This section should not be interpreted as limiting a Producing Party's ability to identify ESI not listed above as being not reasonably accessible because of undue burden or cost pursuant to Fed. R. Civ. P. 26(b)(2)(A).

XI. Privilege and Privilege Logs

A. No Waiver by Disclosure. This Electronic Discovery Order is entered pursuant to Rule 502(d) of the Federal Rules of Evidence. Subject to the provisions of this Electronic Discovery Order, if a Party or subpoenaed non-party (the "Disclosing Party") discloses information in connection with this Action that the Disclosing Party thereafter claims to be privileged or protected by the attorney-client privilege, attorney-work product protection, or any other applicable privilege ("Protected Information"), the disclosure of that Protected Information will not constitute or be deemed a waiver or forfeiture – in this Action or in any other federal or state action – of any claim of privilege or work-product protection that the Disclosing Party would otherwise be entitled to assert with respect to the Protected Information and its subject matter. The

provisions of Federal Rule of Evidence 502(b)(2) are inapplicable to the production of Protected Information under this Order.

B. Notification Requirements; Best Efforts of Receiving Party. A Disclosing Party must notify all prior recipients (“the Receiving Party”) in writing within a reasonable period of time upon learning of the disclosure that such Protected Information was unknowingly disclosed and that the Protected Information was disclosed without intending a waiver by the disclosure. Upon such notification, the Receiving Party must promptly identify and return, sequester, or destroy (or in the case of electronically stored information, delete) the Protected Information and any copies it has and (ii) provide a certification that it will cease further review, dissemination, and use of the Protected Information.

C. Disclosure Motion. If any Receiving Party disagrees that the information is protected from disclosure by the attorney-client privilege, attorney work-product protection, or any other applicable privilege, or asserts that there has been a waiver of privilege, the Receiving Party may keep one (1) copy of the document or thing containing the allegedly Protected Information while it makes a motion to the Court for an order that such information be produced (“Disclosure Motion”). Any Disclosure Motion must be filed under seal. The Disclosure Motion must not assert as a ground for compelling disclosure the fact or circumstances of the disclosure. Pending resolution of the Disclosure Motion, the Receiving Party must not use the challenged information in any way or disclose it to any person other than those required by law to be served with a copy of the sealed Disclosure Motion.

D. Privilege Log. The Parties agree that the following privileged communications or documents need not be included in a privilege log: (a) communications about this action between

Defendants and their counsel, (b) work product of counsel and parties, (c) internal communications within a law firm, (d) communications regarding litigation holds or preservation, collection, or review in this or any litigation, (e) communications about this action between Plaintiffs and their counsel, (f) communications about this action between or among Plaintiffs' counsel, including within a law firm, and (g) communications and documents that post-date filing of the complaint in this action.

XII. Good Faith

The Parties shall make their best efforts to comply with and resolve any differences concerning compliance with this Electronic Discovery Order. If a Producing Party cannot comply with any material aspect of this Electronic Discovery Order, such Party shall inform the Requesting Party as to why compliance with the Electronic Discovery Order was unreasonable or not possible within a reasonable period of time after so learning. No Party may seek relief from the Court concerning compliance with the Electronic Discovery Order unless it has conferred with other affected Parties to the action.

XIII. No Effect on Discovery or Admissibility

This Electronic Discovery Order does not address, limit, or determine the relevance, discoverability, agreement to produce, or admissibility of ESI. The Parties are not waiving the right to seek any discovery, and the Parties are not waiving any objections to specific discovery requests. Nothing in this Electronic Discovery Order shall be interpreted to require disclosure of materials that a Party contends are not discoverable or are protected from disclosure by the attorney-client privilege, the work product doctrine, or any other privilege that may be applicable. Nothing in this Electronic Discovery Order shall be construed to affect the admissibility of any

document or data. All objections to the admissibility of any document or data, except as to the authenticity of the documents produced by a Party as to which that Party stipulates, are preserved and may be asserted at any time.

XIV. Costs and Burden

All Parties reserve the right to seek shifting or sharing of certain discovery costs, including vendor and attorney fees, in appropriate circumstances.

XV. Authenticity

A document produced in this litigation, shall be presumed to be authentic if offered as evidence against the Party that produced it unless the Party (a) gave notice at the time of production that the authenticity of the document may be challenged, including the reasons for such a challenge; or (b) shows good cause for its failure to give such notice at the time of production.

When documents produced in accordance with this Electronic Discovery Order are used in any proceeding herein, including depositions, hearings, or trial, the image copy of documents shall be the copy used. This paragraph does not apply to any Federal Rule of Evidence 1006 summary exhibits or summary demonstratives.

XVI. Protective Order

Nothing in this Electronic Discovery Order shall be deemed to limit, modify, or override any provision of the Protective Order.

XVII. Modification

This Electronic Discovery Order may be modified by (a) a Stipulated Order of the Parties or (b) an Order of the Court for good cause shown.

SO ORDERED, this 6th day of December, 2024.

A handwritten signature in black ink, appearing to read 'R. Lehrburger', written over a horizontal line.

Hon. Robert W. Lehrburger
United States Magistrate Judge